Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132
Telephone: none
Email: none

Daniel David Rigmaiden
Pro Se, Defendant

**UNITED STATES DISTRICT COURT**

**DISTRICT OF ARIZONA**

United States of America,

Plaintiff,

v.

Daniel David Rigmaiden, et al.,

Defendant.

No. CR08-814-PHX-DGC

MOTION TO DISMISS COUNT 72, UNAUTHORIZED ACCESS OF A COMPUTER WITH INTENT TO DEFRAUD, 18 U.S.C. § 1030(a)(4), FOR FAILURE TO STATE AN OFFENSE

Defendant, Daniel David Rigmaiden, appearing *pro se*, respectfully submits *Motion To Dismiss Count 72, Unauthorized Access Of A Computer With Intent To Defraud, 18 U.S.C. § 1030(a)(4), For Failure To State An Offense*. Through this motion, brought under Federal Rules of Criminal Procedure 7(c)(1) and 12(b)(3)(B), the defendant respectfully requests that the Court dismiss count No. 72 of the superseding indictment (Dkt. #200) considering the government failed to state the essential elements of the offense.

## I. INTRODUCTION

As further explained in the *Argument* section, the government failed to sufficiently allege that the unauthorized access of the protected computer owned by a private individual in Glendale, AZ resulted in the obtaining of "anything of value" within the context of 18 U.S.C. § 1030(a)(4). Additionally, the government failed to allege that said access was conducted by "circumventing technological access barriers." The relevant section of the Computer Fraud and Abuse Act ("CFAA"), *i.e.*, 18 U.S.C. § 1030 *et seq.*, reads as follows:

> [(a)] Whoever— [(4)] knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
>
> 18 U.S.C. § 1030(a)(4).

The section of the superseding indictment charging the defendant under 18 U.S.C. § 1030(a)(4) reads as follows:

> 48. The factual allegations in paragraphs 1-47 of this indictment are incorporated by reference and re-alleged as though fully set forth herein.
>
> 49. On or about March 21, 2008, in the District of Arizona and elsewhere, defendant DANIEL DAVID RIGMAIDEN knowingly and with intent to defraud accessed a protected computer used in interstate commerce and communication, without authorization from the computer's owner, a private individual and resident of Glendale, Arizona, and by means of such conduct, including the use of Internet Provider Address XX.XXX.XXX.106, accessed a Meridian Bank business checking account No. XXXXXX0007, which furthered the intended fraud of the United States, committed through the electronic filing of fraudulent income tax returns, and hereby ultimately obtained $68,000 in proceeds from the fraud from the Meridian Bank business checking account No. XXXXXX0007 on or about May 5, 2008.
>
> *Superseding Indictment* (Dkt. #200, p. 32, ¶ 48-49).

"On a motion to dismiss an indictment for failure to state an offense, the court must accept the truth of the allegations in the indictment in analyzing whether a cognizable offense has been charged. The indictment either states an offense or it doesn't." United States v. Boren, 278 F.3d 911, 914 (9th Cir. 2002). "An indictment should be read in its entirety, construed according to common sense, and interpreted to include facts which are necessarily implied." United States v. Lazarenko, 564 F.3d 1026, 1033 (9th Cir. 2009). As further explained below, if accepting the allegations contained in the superseding indictment as truth, count No. 72 fails to allege an offense under all possible interpretations of 18 U.S.C. § 1030(a)(4). Therefore, the relevant section of the superseding indictment does not conform to minimal Constitutional standards and the proper remedy is to dismiss count No. 72 prior to trial. *See* United States v. Gondinez-Rabadan, 289 F.3d 630, 632 (9th Cir. 2002) ("An indictment is fatally defective if it fails to recite an essential element of the charged offense.").

## II. ARGUMENT

### A. The government failed to alleged that the defendant obtained valuable data/information, or something else of value by means of obtaining data/information, from the computer in Glendale, AZ.

As shown by the cases cited in this subsection, courts have found that in order to meet the requirement of obtaining "anything of value" under 18 U.S.C. § 1030(a)(4) a defendant must copy data/information from the protected computer, or use data/information viewed[1] on the protected computer, to further the underlying fraud *and* obtain something of value.[2] In this vein, the thing of value can be the data or information itself (if it holds value) **or** another thing of value (*e.g.*, money) obtained as a *direct result* of exploiting the data or information. Contrary to the reasoning contained in the cases cited immediately below, the government failed to allege that the defendant obtained valuable data or information from the computer owned by the private individual in Glendale, AZ or that he obtained any type of data or information later used to obtain something else of value.[3] Rather, the government alleged that the thing obtained was the government's $68,000 generated "through the electronic filing of fraudulent income tax returns,"[4] an alleged act entirely unrelated to the computer at issue in count No. 72.[5] The relevant point is that a charge under 18 U.S.C. § 1030(a)(4), as a baseline matter, can never survive if the government fails to allege that data/information was obtained from or viewed on the protected computer—unless, of course, the mere use of the computer is valued at $5,000 or more in any 1-year period. *See* 18 U.S.C. § 1030(a)(4).

In *Czubinski*, the First Circuit reversed a conviction under 18 U.S.C. § 1030(a)(4)

[1] While not addressing § (a)(4) specifically, the 1996 amendments to the CFAA note that "the term 'obtaining information' includes merely reading it." S. Rep. No. 104-357, at 7 (1996).

[2] While not at issue here, the statute also permits the thing of value to be "the use of the computer [][if] the value of such use is not more than $5,000 in any 1-year period[.]" 18 U.S.C. § 1030(a)(4).

[3] An example of data/information holding value in and of itself would be a commercial software product. An example of data/information later used to obtain something else of value (*e.g.*, money) would be a client list belonging to a business competitor.

[4] *Superseding Indictment* (Dkt. #200, p. 32, ¶ 49).

[5] *See* fn. No. 9, *infra*.

because "[n]o evidence suggests that [][the defendant] printed out, recorded, or used the information" on the protected computer. United States v. Czubinski, 106 F.3d 1069, 1078 (1st Cir. 1997). The First Circuit analyzed the legislative history and found that "Congress intended section 1030(a)(4) to punish attempts to steal valuable data..." *Id.* *See also* Triad Consultants, Inc. v. Wiggins, 249 Fed. Appx. 38, 40 (10th Cir. 2007) (Under 18 U.S.C. § 1030(a)(4), "[w]e are not persuaded by Triad's argument that the tapes themselves, without access to the information they contain, were 'anything of value.'"); P.C. Yonkers v. Celebrations Superstore, 428 F.3d 504, 509 (3rd Cir. 2005) (Denying claim under 18 U.S.C. § 1030(a)(4) because "[i]t is clear that PC plaintiffs do not know, have not shown, and cannot show, what information, if any, was taken."); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D.Ariz. 2008) ("[T]he plain language of § 1030(a)(2), (4) and (5)(a)(iii) target 'the unauthorized procurement or alteration of information[.]'" (citation omitted)). In the context of obtaining "anything of value" under 18 U.S.C. § 1030(a)(4), count No. 72 of the superseding indictment cannot survive.[6]

### B. Even if obtaining data/information is not required under 18 U.S.C. § 1030(a)(4), the government failed to alleged that the defendant obtained "anything of value" *by means of* accessing the computer in Glendale, AZ.

Contrary to the reasoning in Section II(A), *supra*, the Eleventh Circuit found that the requirement of obtaining "anything of value" under 18 U.S.C. § 1030(a)(4) can be met even if no data/information is obtained from or viewed on the protected computer. In *Barrington*, the court upheld a conviction under 18 U.S.C. § 1030(a)(4) for the fraudulent changing of grades in a University computer database where, by means of such conduct, the defendants obtained unearned credit hours and reimbursed tuition. *See* United States v. Barrington, 648 F.3d 1178 (11th Cir. 2011). Defendants in other courts have also been convicted under 18

[6] The government's general allegation that a bank account was accessed by the defendant from the protected computer is also of no relevance. The government did not allege that the defendant accessed the Meridian Bank computer server without authorization or while exceeding authorized access. Additionally, in relation to the Meridian Bank computer server, the government did not allege that the defendant obtained valuable data/information from the computer, or that data/information was taken or viewed and later used to obtain something else of value.

U.S.C. § 1030(a)(4) without having obtained or viewed data/information on a protected computer—let alone valuable data/information. *See* United States v. Soo Young Bae, 250 F.3d 774 (D.C. Cir. 2001) (printed $525,586 worth of lottery tickets using lottery ticket terminal); United States v. Butler, 16 Fed. Appx. 99 (4th Cir. 2001) (obtained $500 payments for altering credit reports in Equifax computer database); United States v. Philis, 197 Fed. Appx. 76 (2nd Cir. 2006) (obtained payments for changing SSA records in government computer database).

The defendant submits that the conviction in *Barrington*, and the unchallenged convictions[7] in *Soo Young Bae*, *Butler*, and *Philis*, were invalid under 18 U.S.C. 1030(a)(4). However, the issue need not be reached by the Court considering even under *Barrington*, *etc.*, count No. 72 of the superseding indictment fails to allege an offense under 18 U.S.C. 1030(a)(4). Even if applying the above cases, the statute makes clear that the government must allege that the defendant "accesse[d] a protected computer without authorization... and **by means of such conduct**... obtain[ed] anything of value[.]"[8] In each of the cases cited above, a protected computer was accessed, and **by means of such conduct**, the thing of value was obtained. In the present case, however, the superseding indictment alleges that the government's $68,000 in tax refunds was obtained by conduct entirely separate from accessing the computer owned by the private individual in Glendale, AZ.[9] This fatal flaw

[7] By "unchallenged," the defendant means that the defendants' convictions were not challenged based on theories that no offenses were committed under 18 U.S.C. § 1030(a)(4).

[8] 18 U.S.C. § 1030(a)(4) (emphasis added).

[9] The government alleged that the $68,000 in tax refunds—being a part of a larger portion of alleged proceeds—was obtained through the following conduct:

> 17. Commencing on or about an unknown date in January 2008, and continuing through on or about February 12, 2008, a co-conspirator known to the Grand Jury directed a confidential informant working on behalf of the government to open a business checking account, and a shell accounting and tax preparation business entity, in the State of Arizona, on behalf of defendant DANIEL DAVID RIGMAIDEN, and others known and unknown to the Grand Jury, for the purpose of receiving fraudulently obtained income tax refunds from the IRS via electronic funds transfer. A government undercover agent, working with a confidential informant working on behalf of the government, subsequently opened Meridian Bank business checking account No. XXXXXX0007, in Phoenix, Arizona, on behalf of, and at the direction of, defendant DANIEL DAVID RIGMAIDEN, and others known and unknown to the Grand Jury, for the subject purpose.
>
> 18. Commencing on or about March 3, 2008, and continuing until on or about April

requires dismissal of count No. 72 even if the Court rejects the defendant's argument in Section II(A), *supra*. In the context of *Barrington*, an easy way to decide the issue is to examine whether the $68,000 loss can still be realized *but-for* the alleged access to the computer in Glendale, AZ. Because the superseding indictment clearly answers this question in the affirmative,[10] accessing the computer in Glendale, AZ was not conduct acting as a means by which the $68,000 was obtained. Therefore, count No. 72 must be dismissed.

The government is attempting to satisfy the essential elements of the offense by grafting its interest in the $68,000 onto the private interests of the individual who owns the computer in Glendale, AZ.[11] While there is no criminal case law addressing the government's incorrect use of the statute in this context, the civil implications of 18 U.S.C. § 1030, *et seq.*[12] offer some insight into the issue. Note: even if a "case arises in a civil context, [][a court's] interpretation of §§ 1030(a)(2) and (4) is equally applicable in the criminal context." LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009).

15, 2008, defendant DANIEL DAVID RIGMAIDEN, and others known and unknown to the Grand Jury, electronically filed and caused to be electronically filed, approximately 361 false claims upon the United States via fraudulent income tax returns filed with the IRS, and thereby fraudulently sought the payment of approximately $668,876.00 in income tax refund on behalf of deceased individuals, via electronic funds transfers, into Meridian Bank business checking account No. XXXXXX0007, in Phoenix, Arizona.

19. During the period beginning on or about March 3, 2008, and continuing through on or about April 4, 2008, defendant DANIEL DAVID RIGMAIDEN, and others known and unknown to the Grand Jury, caused the Austin Financial Center, Financial Management Services, Austin, Texas, to transfer, via electronic funds transfers, approximately $447,407.00 in fraudulently generated income tax refunds into Meridian Bank business checking account No. XXXXXX0007, in Phoenix, Arizona.

…

44. On or about May 5, 2008, defendant DANIEL DAVID RIGMAIDEN picked up a Federal Express package containing $68,000.00 of fraudulently obtained income tax refunds, previously deposited in Meridian Bank business checking account No. XXXXXX0007, in Phoenix, Arizona, from a commercial mail receiving agency located in the State of California.

*Superseding Indictment* (Dkt. #200, p. 6-7 and 14, ¶¶ 17-19 and 44).

[10] *See* fn. No. 9, *supra*.

[11] This is similar to the Court grafting the interests of alleged identity fraud victims (who are deceased) onto the interests of Domicilio, Verizon, and Lenovo—entities that were defrauded of nothing and lost nothing—in an attempt to distinguish controlling Ninth Circuit precedent. *See* Dkt. #1009.

[12] "Any person who **suffers damage or loss** by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief...." 18 U.S.C. § 1030(g) (emphases added).

Because the private individual and resident of Glendale, AZ did not suffer the government's "damage or loss" of $68,000, he/she would be unable to rely on the facts alleged at Dkt. #200, p. 32, ¶ 48-49 to state a claim for damages under 18 U.S.C. §§ 1030(a)(4) and (g).[13] Similarly, the government cannot satisfy the essential elements of the offense by grafting the Glendale, AZ resident's interest in his/her computer onto the government's interests in the $68,000. In the context of a civil claim, the Ninth Circuit indicated that a third-party (*i.e.*, not the computer's owner) may bring a valid claim for damages under 18 U.S.C. § 1030(g) if the third-party stores data on the protected computer. *See* Theofel v. Farey Jones, 341 F.3d 978, 986 (9th Cir. 2003) ("Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it."); *see also* Nexans Wires S.A., 319 F. Supp. 2d at 472 ("Because plaintiffs store their information on AEB and ASW computers they may suffer the type of harm contemplated by the statute if those computers are damaged."). In the present case, however, the government was not storing information on the Glendale, AZ resident's computer and, even if it was, there was no allegation of said information being accessed or obtained by the defendant.

Somewhat separate from the government's failure to state an offense, the legislative history for the CFAA shows that lawmakers sought to prevent the government from using 18 U.S.C. § 1030(a)(4) to charge crimes based on the type of conduct alleged in count No. 72:

> The Committee was concerned that computer usage that is wholly extraneous to an intended fraud might nevertheless be covered by this subsection if the subsection were patterned directly after the current mail fraud and wire fraud laws. If it were so patterned, the subsection might be construed as covering an individual who had devised a scheme or artifice to defraud solely because he used a computer to keep records or to **add up [the] potential "take" from the crime**. The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the commission or execution of the fraud.
>
> S. Rep. No. 99-432 at 9 (1986) (emphasis added), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2487.

[13] However, even if the $68,000 loss could somehow be grafted onto the interests of the resident in Glendale, AZ., "there is nothing [in the legislative history] to suggest that the 'loss' or costs alleged can be unrelated to the computer." Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004).

The Ninth Circuit held that "[a]n indictment should be... interpreted to include **facts** which are necessarily implied." Lazarenko, 564 F.3d at 1033 (emphasis added). While not specifically stated in the indictment, the government alleges that the defendant used someone's personal computer without authorization for the purpose of logging into a web based bank account portal so that he could merely view transactions corresponding to allegedly fraudulent tax refunds.[14] This is very similar to using a computer to add up the potential "take" from a crime. "While such a tenuous link might be covered under current law where the instrumentality used is the mails or the wires, the Committee does not consider that link sufficient with respect to computers. To be prosecuted under this subsection, the use of the computer must be more **directly linked** to the intended fraud." S. Rep. No. 99-432 at 9 (1986) (emphasis added).

### C. The government failed to alleged that the defendant obtained use of the computer in Glendale, AZ with said use being valued at $5,000 or more in any 1-year period.

Because the government only alleged *use* of the computer in Glendale, AZ, "the object of the fraud and the thing obtained consists only of the use of the computer..."[15] The facts alleged in the superseding indictment only satisfy the fraud element[16] of 18 U.S.C. § 1030(a)(4) in the effect that mere access qualifies as the "intended fraud." *See* Ebay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D.Cal. 2009) ("'fraud' under the CFAA only requires a showing of unlawful access;"). The thing of value can then only be the mere use of the Glendale, AZ computer but the government failed to allege that such use had a value of $5,000 or more in any 1-year period—as required by 18 U.S.C. § 1030(a)(4).

[14] For example, during the March 28, 2013 motions hearing, the government alleged that "[t]he defendant also used the computer and the aircard to move through a personal computer in a residence in Arizona in order to check the balance on one of the bank accounts that was involved in the fraud." *March 28, 2013 Motions Hearing Transcripts*, p. 84, ln 19-22.

[15] 18 U.S.C. § 1030(a)(4).

[16] The element, "knowingly and with intent to defraud," is analyzed under "the same standard used for 18 U.S.C. 1029 relating to credit card fraud." S. Rep. No. 99-432 at 10 (1986). In the context of 18 U.S.C. § 1029: "'With intent to defraud' means that the offender has a conscious objective, desire or purpose to deceive another person, and to induce such other person, in reliance upon such deception, to assume, create, transfer, alter or terminate a right, obligation, or power with reference to property." S. Rep. No. 368 at 7, *reprinted in* U.S.C.C.A.N. 3647, 3652.

In the context of obtaining the mere use of the computer under 18 U.S.C. § 1030(a)(4), count No. 72 of the superseding indictment cannot survive.

### D. The government failed to alleged that the defendant accessed the protected computer by circumventing technological access barriers.

The government failed to allege that the defendant circumvented technological access barriers in order to gain access to the protected computer in Glendale, AZ. In *Nosal*, the Ninth Circuit addressed a challenge horizontal to the defendant's and noted that 18 U.S.C. § 1030(a)(4) of the CFAA has a "general purpose [] to punish hacking — the circumvention of technological access barriers[.]" United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012). While nothing in the text of 18 U.S.C. § 1030(a)(4) states that circumventing technological access barriers is an essential element of the offense, the Ninth Circuit held in *Jackson* that "implied, necessary **elements**, not present in the statutory language, must be included in an indictment." United States v. Jackson, 72 F.3d 1370, 1380 (9th Cir. 1995) (emphasis added). Because this implied, necessary element is not present, count No. 72 of the superseding indictment cannot survive.

* * * * *

The facts alleged by the government at Dkt. #200, p. 32, ¶ 48-49 fail to allege an offense under any possible application of the statute. Therefore, the defendant respectfully requests that the Court dismiss count No. 72 for failure to state an offense.

This motion was drafted by the *pro se* defendant, however, he authorizes his shadow counsel, Philip Seplow, to file this motion on his behalf using the ECF system.

LRCrim 12.2(a) requires the following text in motions: "Excludable delay under 18 U.S.C. § 3161(h)(1)(D) will occur as a result of this motion or of an order based thereon."

///

///

///

///

///

Respectfully Submitted: May 13, 2013

PHILP SEPLOW, Shadow Counsel, on
behalf of DANIEL DAVID RIGMAIDEN,
Pro Se Defendant:

s/ Philip Seplow
Philip Seplow
Shadow Counsel for Defendant.

## CERTIFICATE OF SERVICE

I hereby certify that on: May 13, 2013 I caused the attached document to be electronically transmitted to the Clerk's Office using the ECF system for filing and transmittal of a Notice of Electronic Filing to the following ECF registrants:

Taylor W. Fox, PC
Counsel for defendant Ransom Carter
2 North Central Ave., Suite 735
Phoenix, AZ 85004

Frederick A. Battista
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

Peter S. Sexton
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

James R. Knapp
Assistant United States Attorney
Two Renaissance Square
40 North Central Ave., Suite 1200
Phoenix, AZ 85004

By: s/ Daniel Colmerauer
(Authorized agent of Philip A. Seplow, Shadow Counsel for Defendant; See ECF Proc. I(D) and II(D)(3))